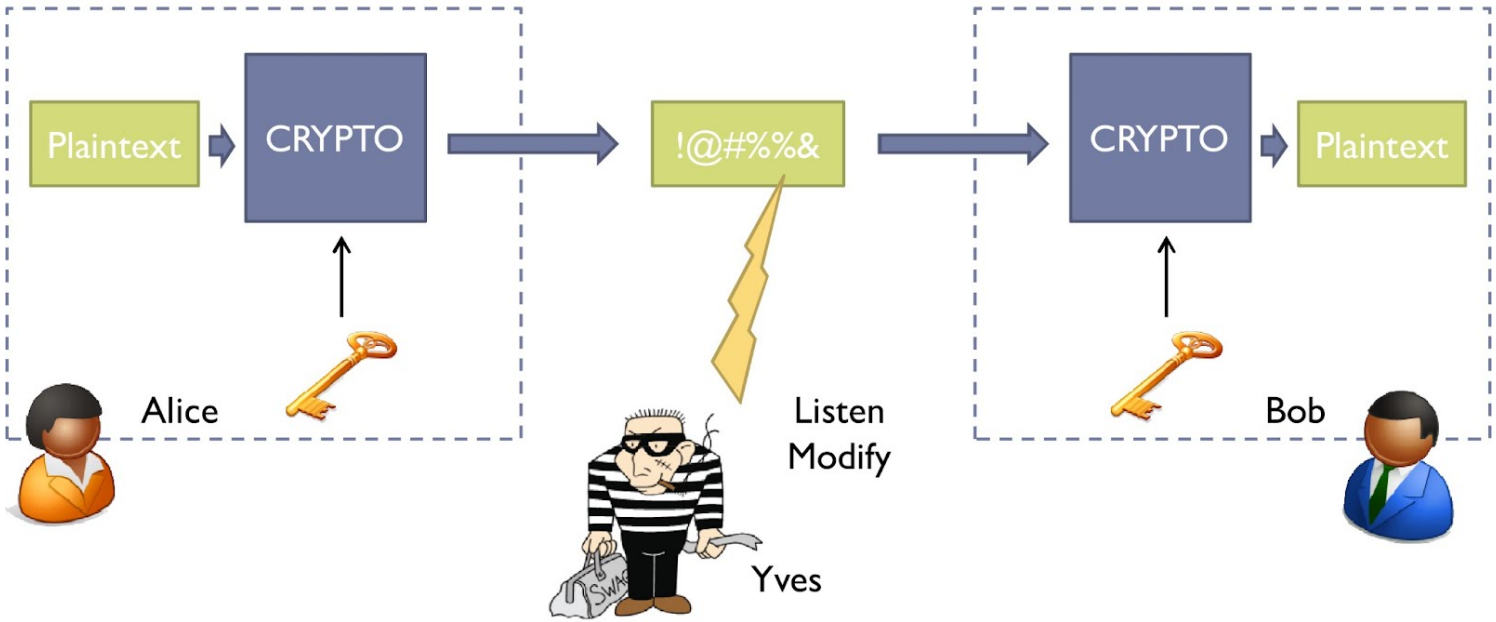
Cryptanalyse à l'ère préinformatique

François Ducrot
Université d'Angers

ANF Angers 2014

Schéma général



Position du problème

On va se placer pour une fois dans la peau du méchant

Bonnes pratiques du codeur

- Ne pas se reposer sur le secret de l'algorithme de codage
- Ne jamais coder deux messages avec la même clé
- Ne jamais coder le même message avec deux clés différentes
- Ne pas croire que le pseudo-aléatoire est non prédictible

Bonnes pratiques du codeur

- Ne pas se reposer sur le secret de l'algorithme de codage
- Ne jamais coder deux messages avec la même clé
- Ne jamais coder le même message avec deux clés différentes
- Ne pas croire que le pseudo-aléatoire est non prédictible

`Exploiter le non respect de ces quelques règles.

Exemple historique : code de César

On décale chaque lettre d'un certain nombre de crans (ici 5) dans l'alphabet.

a	b	c	d	e	...	v	w	x	y	z
e	f	g	h	i	...	z	a	b	c	d

BONJOUR est transformé en FSRNSYV

Le code de César

Exercice : Décryptez le message

PXIRQIBPXJFP

Le code de César

Exercice : Décryptez le message

PXIRQIBPXJFP

Solution : on teste les différents décalages :

- `PXIRQIBPXJFP`

Le code de César

Exercice : Décryptez le message

PXIRQIBPXJFP

Solution : on teste les différents décalages :

- `PXIRQIBPXJFP`
- `QYJSRJCQYKGQ`

Le code de César

Exercice : Décryptez le message

PXIRQIBPXJFP

Solution : on teste les différents décalages :

- PXIRQIBPXJFP
- QYJSRJCQYKGQ
- RZKTSKDRZLHR

Le code de César

Exercice : Décryptez le message

PXIRQIBPXJFP

Solution : on teste les différents décalages :

- PXIRQIBPXJFP
- QYJSRJCQYKGQ
- RZKTSKDRZLHR
- SALUTLESAMIS

Le code de César

Exercice : Décryptez le message

PXIRQIBPXJFP

Solution : on teste les différents décalages :

- PXIRQIBPXJFP
- QYJSRJCQYKGQ
- RZKTSKDRZLHR
- SALUTLESAMIS

On vient de casser ce code par une attaque par force brute, ce qui est possible car, une fois qu'on connait l'algorithme de codage, le nombre de clés à envisager est très faible (25).

Codes mono-alphabétiques

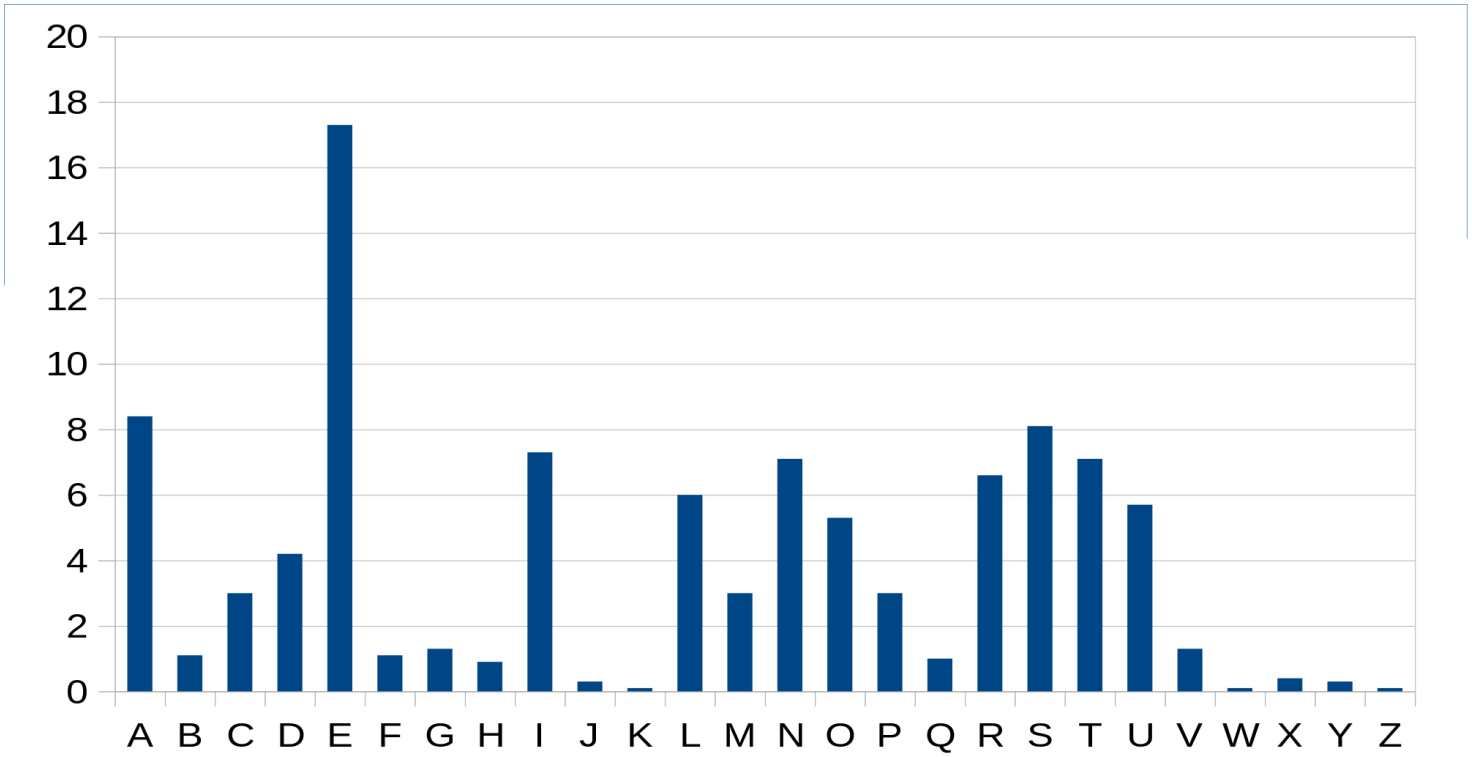
- Le chiffre de César est appelé mono-alphabétique. Il repose sur un correspondance lettre $\leftrightarrow$ lettre.
- La clé d'un code mono-alphabétique est une table :

a	b	c	...	x	y	z
g	v	a	...	u	b	m

- Il y a $26\,! = 403291461126605635584000000$ clés possibles.
- Une attaque exhaustive par force brute, en testant successivement tous les codes mono-alphabétiques n'est pas envisageable.
- Mais on le casse facilement par analyse de fréquence.

Analyse fréquentielle

Dans une langue donnée les lettres apparaissent avec des fréquences différentes. Par exemple en français :



Exercice

Décryptez le cryptogramme suivant, obtenu en appliquant un code mono-alphabétique à un texte français :

bgnkxyuze py uy eqwe mgqmdy fy tgnny dyqly zhlrgwe h zywny uh tgqkwy yxywnxy uye oyqv ey ryluhwynx ew jwxy sqy py n hjhwe zhe by xyuze fy uy fwly py u ynfgle yx qny fyuw dyqly hzlye bh zyneyy sq wb yxhwx xyuze fy mdylmdyl by eguuywb u yjywbbhwx py jgqbhwe zgeyl by jgbquy sqy py mlgohwe hjgwl ynmgly fhne bye uhwne yx egqrrbyl uh bquwyly py n hjhwe zhe myeey yn fgluhnx fy rhwly fye lyrbyvwgne eql my sqy py jynhwe fy rhwly uhwe mye lyrbyvwgne hjhwynx zlwe qn xgql qn zyq zhlxwmqbwyl wb uy eyutbhwxx sqy p yxhwe ugw uyuy my fgnx zhlbhwx b gqjlhky qny ykbwey qn sqhxqgl bh lwjhbwxy fy rlhnmgwe zlyuwyl yx fy mdhlbye sqwnx myxxy mlgohnmy eqljwjhwx zynfhnx sqybsqye eymgnfye h ugn lyjywb ybby ny mdgsqhwx zhe uh lhwegn uhwe zyehwx mguuy fye ymhwbbye eql uye oyqv yx bye yuzymdhwx fy ey lynfly mguzxy sqy by tgqkygwl n yxhwx zbqe hbbquy zqwe ybby mguuynmhwx h uy fyjynwl wnwnxybbwkwtby mguuy hzlye bh uyxyuzeomgey bye zyneyye f qny yvwexynmy hnxylwyqly by eqpyx fq bwjly ey fyxhmdhwx fy ugw p yxhwe bwtly fy u o hzzbwsqyl gq ngn hqeewxgx py lymgqjlhwe bh jqy yx p yxhwe twyn yxgnny fy xlgqjyl hqxgql fy ugw qny gtemqlwxy fgqmy yx lyzgehnxy zgql uye oyqv uhwe zyqx yxly zbqe ynmgly zgql ugn yezlwx h sqw ybby hzzhlhweehwx mguuy qny mdgey ehne mhqey wnmguzlydynewtby mguuy qny mdgey jlhwuynx gtemqly py uy fyuhnfhwe sqybby dyqly wb zgqjhwx yxly p ynxynfhwe by ewrrbyuynx fye xlhwne sqw zbqe gq ugwne ybgwkny mguuy by mdhnx f qn gweyhq fhne qny rglyx lybyjhnx bye fwexhnmye uy fymlwjhwx b yxynfqy fy bh mhuzhkny fyeylxy gq by jgohkyql ey dhxy jyle bh exhxwgn zlgmdhwny yx by zyxwx mdyuwn sq wb eqwx jh yxly klhjy fhne egn egqjynwl zhl b yvmwxhxwgn sq wb fgwx h fye bwyqv ngqjyhqv h fye hmxye wnhmmgqxquye h bh mhqeylwy lymynxy yx hqv hfwyqv egqe bh bhuzy yxlhnkyly sqw by eqwjynx ynmgly fhne by ewbynmy fy bh nqwx h bh fgqmyql zlgmdhwny fq lyxgql

Pour nous aider

Pourcentage d'apparition des lettes en français

E	A	S	I	N	T	R	L	U	O	D	C	M
17.3	8.4	8.1	7.3	7.1	7.1	6.6	6.0	5.7	5.3	4.2	3.0	3.0

et dans notre texte :

Y	H	W	E	Q	N	X	L	G	B	U	M	F
19.0	7.9	7.7	7.6	6.4	6.1	6.1	5.8	5.3	5.2	4.3	3.7	3.2

Bigrammes de lettres redoublées en français (sur 10000)

SS	EE	LL	TT	NN	MM	RR	PP	FF	CC
73	66	66	29	24	20	17	16	10	8

Nombre de bigrammes de lettres redoublées dans le texte

YY	BB	EE	UU	XX	RR	NN	ZZ	MM
11	8	7	7	3	2	2	2	1

Les codes poly-alphabétiques

Vous venez de prouver qu'un code mono-alphabétique est facilement cassé par analyse fréquentielle.
C'est pourquoi on regarde des codes poly-alphabétiques.

- Les lettres sont regroupées par blocs de k lettres. On utilise une table qui fait correspondre un bloc de k lettres à un autre. Par exemple avec $k = 3$:

aaa	aab	abc	...
ubd	icz	dja	...

- Combien de clés possibles ?
  - 26 lettres (ou 128 caractères en ASCII)
  - $n = 26^k$ (ou 128^k) blocs de k caractères
  - $(26^k)!$ (ou $(128^k)!$) clés possibles !
- Un code donné utilise seulement une partie de cette immense ensemble de clés

Le code de Vigenère (XVI-ème siècle)

- Une table d'addition pour les lettres

	a	b	c	d
a	a	b	c	d
b	b	c	d	e
c	c	d	e	f
d	d	e	f	g

- On ajoute la clé (ici "abc") au texte en clair

clair	b	o	n	j	o	u	r	l	e	s	a	m	i	s
clé	a	b	c	a	b	c	a	b	c	a	b	c	a	b
crypté	b	p	p	j	p	w	r	m	g	s	b	p	i	t

- C'est un code multi-alphabétique : s a été codé une fois en s et une fois en t.

Cryptanalyse du code de Vigenère (XIX-ème siècle)

- Deviner la longueur de la clé en observant des répétitions
- Une fois qu'on connait la longueur de la clé (par exemple 3), on regarde les trois sous-messages constitués des lettres en positions
  - 1,4,7,10,13,...
  - 2,5,8,11,14,...
  - 3,6,9,12,15,...
- Chacun est codé par un code de César. Trop facile !

Masque jetable : le code de Vernam

- On remplace la séquence abcabcabc par une suite aléatoire infinie de lettres.
- Chaque portion de la clé n'est alors utilisée qu'une seule fois

Masque jetable : le code de Vernam

- On remplace la séquence abcabcabc par une suite aléatoire infinie de lettres.
- Chaque portion de la clé n'est alors utilisée qu'une seule fois
-  Théoriquement incassable !

Masque jetable : le code de Vernam

- On remplace la séquence abcabcabc par une suite aléatoire infinie de lettres.
- Chaque portion de la clé n'est alors utilisée qu'une seule fois
-  Théoriquement incassable !
- À condition que
  - la clé soit vraiment non prédictible
  - on sache communiquer la clé au préalable !

La machine enigma

- Utilisée par l'armée allemande dès 1925
- Machine électromécanique constituée de :
  - un clavier
  - des voyants lumineux
  - un tableau de brassage
  - des roues codeuses
  - un réflecteur
- Quand on presse une touche, l'électricité suit un certain chemin, et éclaire un voyant.
- La clé est constituée des positions des roues codeuses et du tableau de brassage

Les roues codeuses (rotors)

26 contacts électriques sur chaque face, et un réseau de fils électriques reliant les contacts d'une face à ceux de l'autre face

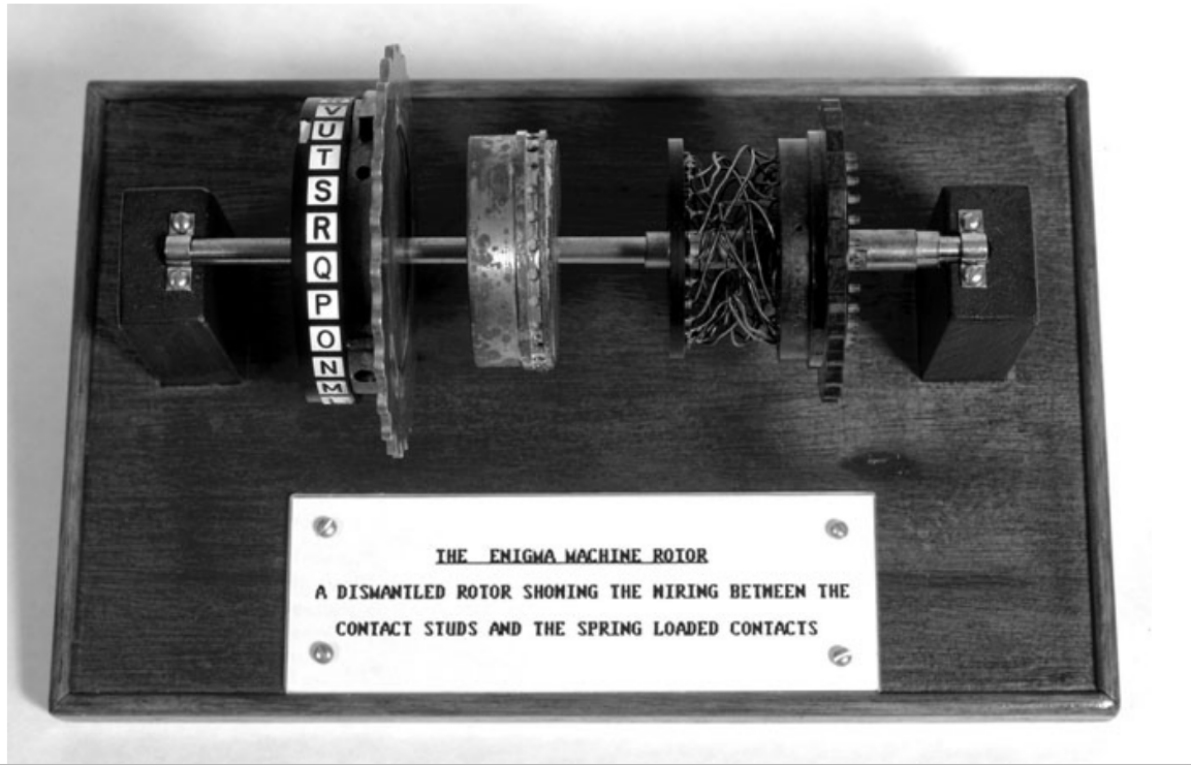
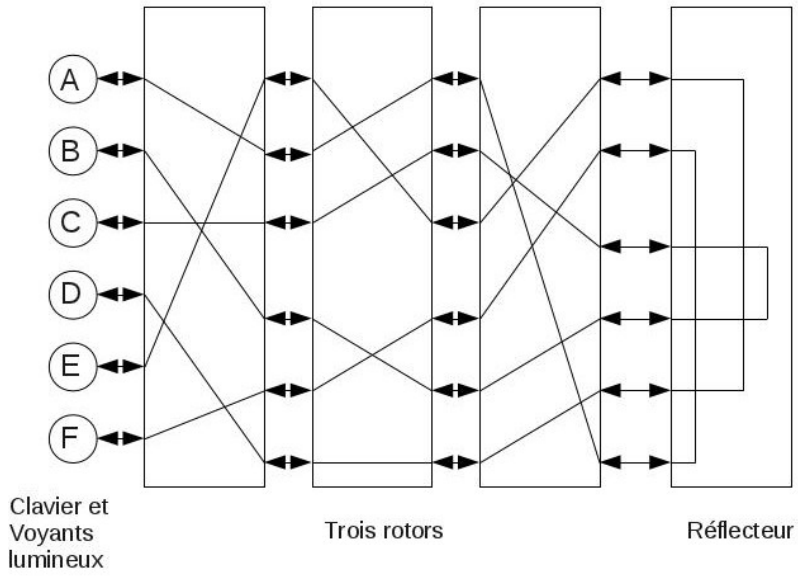


Schéma très très simplifié d'enigma



- Quand on tape sur la touche A, le voyant F s'allume.
- Et inversement !
- Donc la même machine code et décode.

Un peu moins simplifié

- Comme décrit précédemment, il s'agirait d'un code monoalphabétique. On introduit un phénomène supplémentaire.
- A chaque pression sur une touche la roue de gauche tourne d'un 26-ème de tour
- Quand la roue de gauche a fait un tour, la roue du milieu tourne d'un 26-ème de tour, et ...
- Donc, en réalité, la machine code des séquences de $26^3 = 17576$ lettres. Elle est fortement poly-alphabétique.

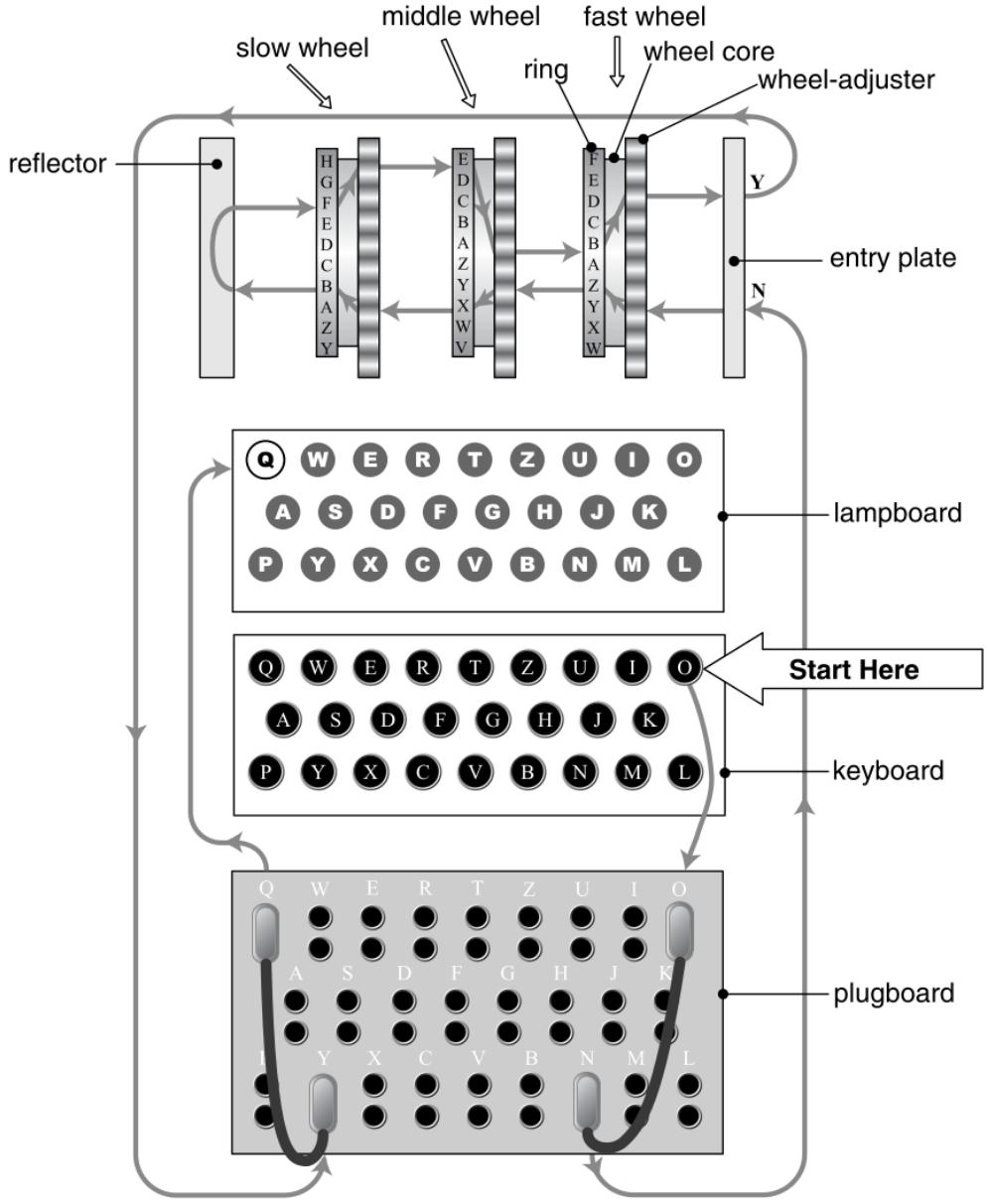
Un peu moins simplifié

- Comme décrit précédemment, il s'agirait d'un code monoalphabétique. On introduit un phénomène supplémentaire.
- A chaque pression sur une touche la roue de gauche tourne d'un 26-ème de tour
- Quand la roue de gauche a fait un tour, la roue du milieu tourne d'un 26-ème de tour, et ...
- Donc, en réalité, la machine code des séquences de $26^3 = 17576$ lettres. Elle est fortement poly-alphabétique.
- Mais le nombre de clés (les 17576 positions possibles des roues) est bien trop faible

Encore un peu moins simplifié

- On introduit entre le clavier et les rotors, ainsi qu'entre les rotors et les voyants, un tableau de brassage constitué de 10 fils qui échangent chacun un couple de lettres.
- Le nombre de brassages possibles est 150738274937250
- On mélange donc une partie fortement multi-alphabétique avec peu de clés et une partie mono-alphabétique avec beaucoup de clés.
- En tout $17576 \times 150738274937250 \simeq 2,6\ 10^{18}$ clés.

Schéma presque complet



Déploiement et mise en oeuvre

- Déployée massivement par l'armée allemande pendant la seconde guerre mondiale
- A joué un rôle décisif pendant la bataille de l'atlantique
- Un opérateur qui tape, un qui note la sortie des voyants, un opérateur radio qui envoie en morse
- Des carnets de code donnant la clé du jour (brouilleur + tableau)

Mode opératoire

A chaque fois que l'opérateur envoie un message :

- l'opérateur règle la machine suivant la clé du jour
- il choisit un groupe de trois lettres (indicatif de message), définissant de nouvelles positions des rotors
- il code cet indicatif avec la clé du jour
- il règle les rotors avec l'indicatif du message, puis code le corps du message avec la nouvelle position des rotors

Le message transmis comprend donc :

- l'indicatif de trois lettres, codé avec la clé du jour
- le corps du message codé avec l'indicatif

Premières attaques

Pendant les années 30, le code enigma a d'abord mis en échec les cryptanalystes, mais

- espionnage classique des services secrets français qui récupèrent une partie de la documentation technique et des carnets de codes
- cryptanalyse réalisée par les services secrets polonais, en exploitant en particulier une erreur de procédure : pour éviter les erreurs de transmissions, les trois lettres de l'indicatif étaient codées deux fois, donc avec des positions des roues différentes les deux fois.
- jusque vers 1938, les services secrets polonais étaient en mesure de décoder tous les messages codés par enigma
- ensuite, les allemands ont rectifié cette erreur de procédure et ont complexifié les machines enigma : tout était à refaire.

La cryptanalyse polonaise

En récoltant les indicatifs des différents messages interceptés pendant une journée

	lettre 1	lettre 2	lettre 3	lettre 4	lettre 5	lettre 6
Message 1	F	K	R	P	H	T
Message 2	U	S	Q	C	U	D
Message 3	F	A	N	P	B	Q
Message 4	L	W	Q	J	R	D

On voit que tous les messages ayant F en lettre 1 ont P en lettre 4.
On établit alors une correspondance :

lettre 1	A	B	C	D	E	F	G	H	I	J	K	L	M
lettre 4	Z	N	H	G	O	P	A	S	W	Y	T	J	Q
lettre 1	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
lettre 4	B	F	D	X	E	I	K	C	U	V	M	L	R

Correspondances analogues entre les lettres 2→5 et 3→6

La cryptanalyse polonaise

En suivant les correspondances :

$A \to Z \to R \to E \to O \to F \to P \to D \to G \to A$

$C \to H \to S \to I \to W \to V \to U \to C$

$J \to Y \to L \to J \quad , \quad M \to Q \to X \to M$

$B \to N \to B \quad , \quad K \to T \to K$

On voit ici apparaitre des cycles de longueurs 9,7,3,3,2,2.

On aurait pu faire de même avec les lettres 2 et 5 ainsi que 3 et 6.

Du fait de la structure particulère du tableau de brassage, quand on règle différemment le tableau sans modifier le brouilleur, les nombres de cycles et leurs longueurs auraient été les mêmes.

La cryptanalyse polonaise

Principe de l'attaque :

- Etablir la structure de cycle à partir des messages interceptés
- Essayer les 17576 combinaisons du brouilleur, pour trouver lesquelles sont compatibles avec cette structure
- Pour chacune de ces positions, appliquer à un message la machine enigma (sans tableau de brassage).
- Le texte obtenu n'est alors pas encore intelligible, mais il est maintenant codé de manière mono-alphabétique.
- Utiliser des méthodes manuelles pour le décoder.

La cryptanalyse polonaise

Principe de l'attaque :

- Etablir la structure de cycle à partir des messages interceptés
- Essayer les 17576 combinaisons du brouilleur, pour trouver lesquelles sont compatibles avec cette structure
- Pour chacune de ces positions, appliquer à un message la machine enigma (sans tableau de brassage).
- Le texte obtenu n'est alors pas encore intelligible, mais il est maintenant codé de manière mono-alphabétique.
- Utiliser des méthodes manuelles pour le décoder.

L'attaque a été rendue possible par :

- une erreur de conception structurelle du tableau de brassage
- une erreur de procédure (coder deux fois un même texte avec deux clés)

A partir de l'invasion de la Pologne en 1939, ce sont les services secrets britanniques qui mènent l'essentiel de la cryptanalyse de Enigma.
Les services de cryptanalyse sont concentrés dans le manoir de Bletchley Park

Ils regroupent de nombreux mathématiciens, dont Alan Turing

La Méthode du mot probable

On peut deviner que certaines chaînes de caractères se trouveront dans des messages

- Mots ou expressions prévisibles par exemple : WETTERVORHERSAGE, GEHEIME, ...
- Susciter la chance : miner une zone maritime ; des messages seront sans doute envoyés pour signaler le champ de mines.

On cherche à trouver quel zone d'un texte chiffré peut correspondre à ce mot probable en exploitant un défaut de conception de la machine Enigma :

Jamais une lettre n'est codée en elle même

La Méthode du mot probable

On pense que la chaîne de caractères probable WETTERVORHERSAGEBISKAYA apparait de manière codée dans le chaîne QFZWRWIVTYRESXBFOGKUHQBAISEZ.

On teste les coïncidences, en décalant à chaque fois

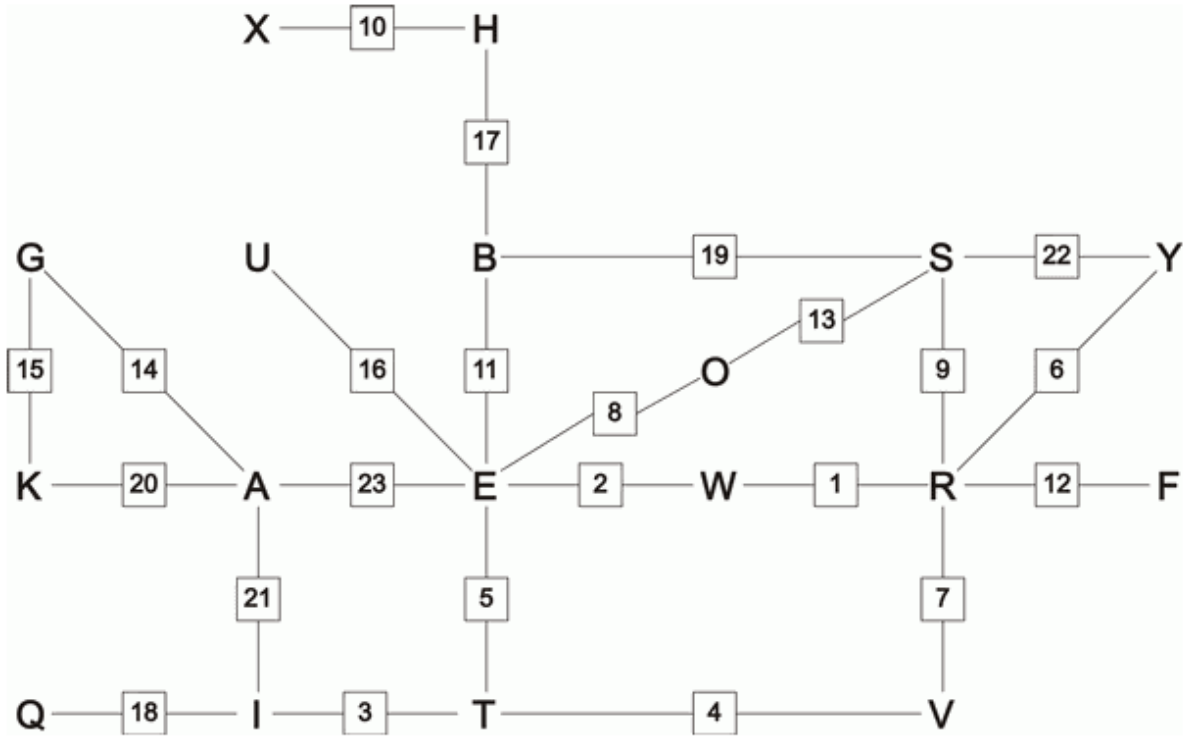
Q	F	Z	W	R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S	K
	W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S
		W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I
			W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B
				W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E

On peut donc envisager que la bonne correspondance soit :

1	2	3	4	5	6	7	8	9	11	12	13	14	15	16	17	18	19	20
R	W	I	V	T	Y	R	E	S	X	B	F	O	G	K	U	H	Q	B
W	E	T	T	E	R	V	O	R	H	E	R	S	A	G	E	B	I	S

La Méthode du mot probable

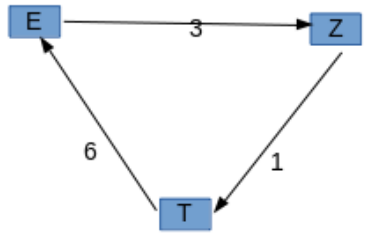
Ce qui peut être schématisé par le diagramme (appelé un menu)



Si on modifie le réglage du tableau en laissant les rotors inchangés, on garde le même menu (seules les lettres sont remplacées par d'autres). Un menu caractérise donc la disposition des rotors.

Tester un menu

Si le menu contient le motif suivant :



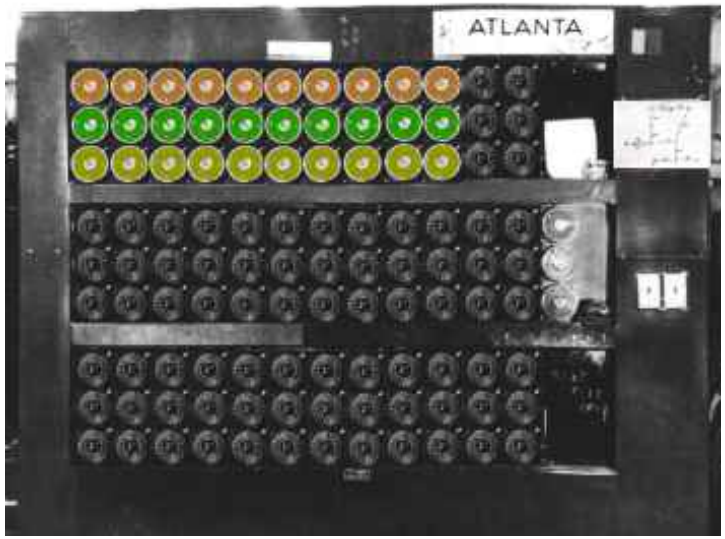
Si on note E', T', Z' les lettres qui correspondent à E, T, Z après le passage dans tableau de brassage, le diagramme signifie que :

- le brouilleur, en position initiale , envoie Z' sur T'
- le brouilleur, avancé de 5 positions, envoie T' sur E'
- le brouilleur, avancé de 2 positions, envoie E' sur Z'

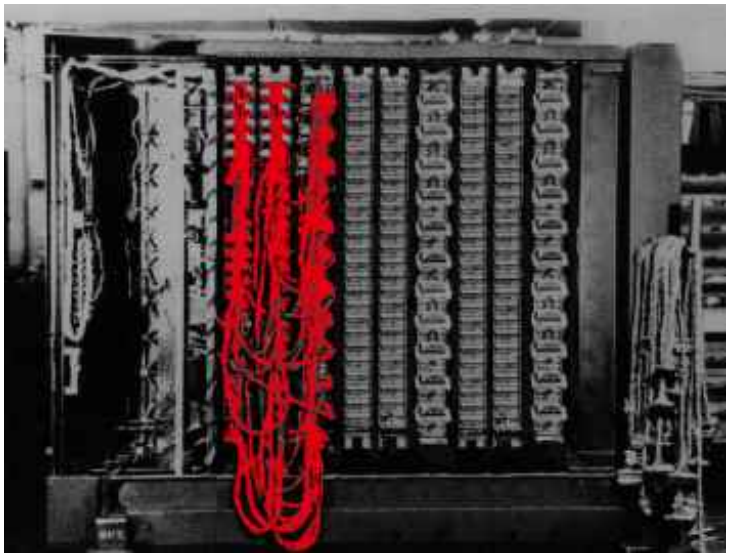
Il suffit de mettre en série électriquement trois brouilleurs, en position n, $n+5$ et $n+2$ et de voir si il se forme une boucle pour une valeur de n.

Les bombes de Turing

- Machine électro-mécanique destinées à déterminer quelles configurations des rotors sont compatibles avec un schéma donné



face avant



face arrière

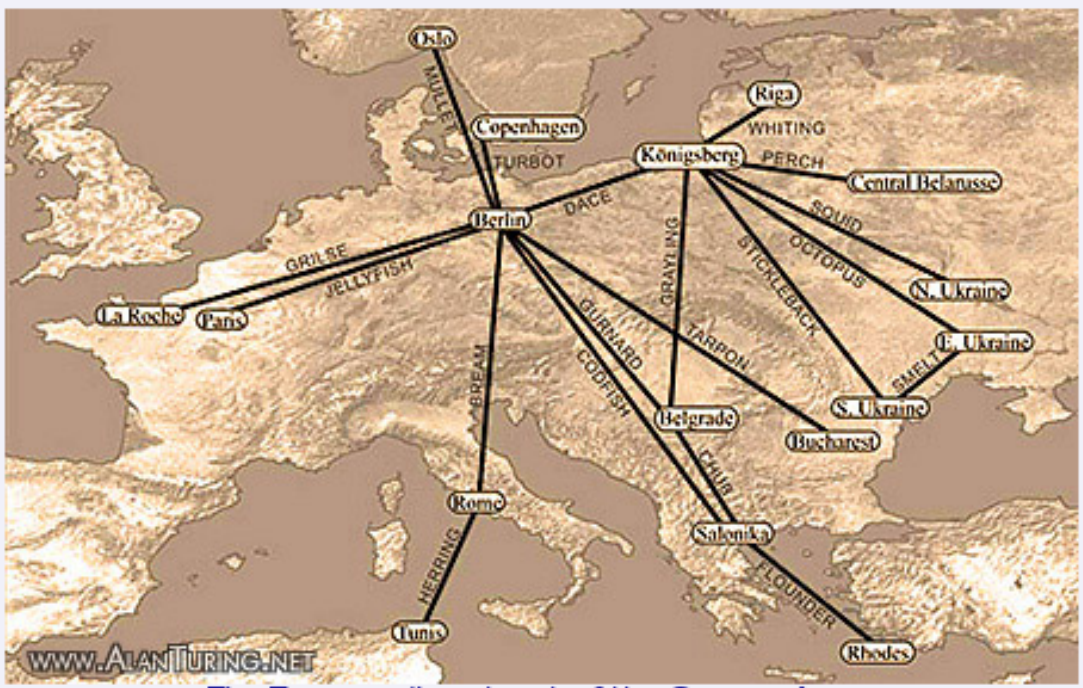
- Chaque colonne de 3 tambours émule une machine enigma, chacune décalée d'une lettre par rapport à la précédente
- Le câblage arrière est constitué de câbles à 26 brins et reconstituent le menu à tester.

Les bombes de Turing

- Les tambours sont entrainés par un moteur, et testent successivement toutes les positions des machines enigma.
- Lorsque une position correspond au menu testé, le courant passe dans le câblage et active un relai.
- Les tambours rapides tournent à environ 200 trs/min. Les 17576 configurations peuvent être testées en environ 1h30.
- La “programmation” d’une bombe consistait en les branchements qui traduisaient physiquement le menu. Ces branchements devaient être vérifiés par plusieurs opérateurs, avant de lancer une session.
- Plusieurs centaines de bombes ont été construites, d’abord par les anglais, puis par les américains, et ont permis vers la fin de la guerre de déchiffrer presque systématiquement les messages allemands codés par enigma.

Le code Tunny

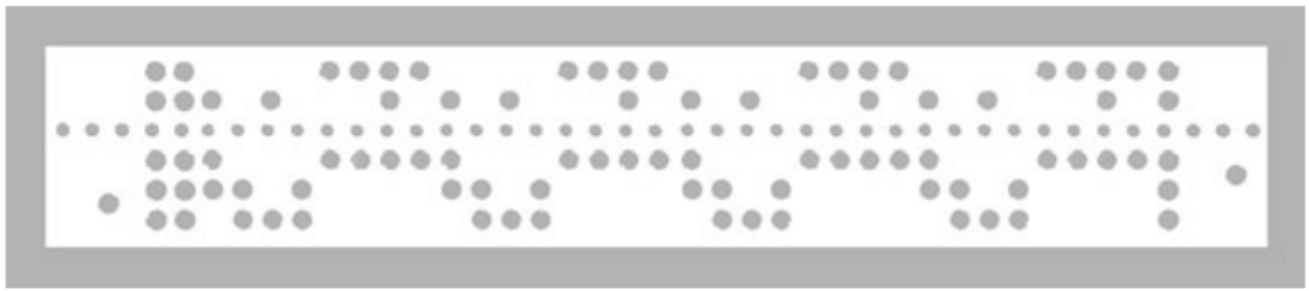
- Certaines communications de l'état major allemand ont été codées par d'autres systèmes basés sur un système de téléscripteurs codés en temps réel.
- Les alliés dénommaient les les différents codes de cette famille par des noms de poissons (tunny, sturgeon, ...)



The Tunny radio network of the German Army,
March 1943 – July 1944.7

Principe du téléscripteur publique

- L'opérateur tape le texte sur un clavier.
- Chaque lettre est codée (par un code international) sur 5 bits par une machine, qui envoie le message par radio, sous forme de 5 flux de signaux impulsion/plat.
- La machine réceptrice traduit ce flux de données et imprime directement la sortie en texte clair.

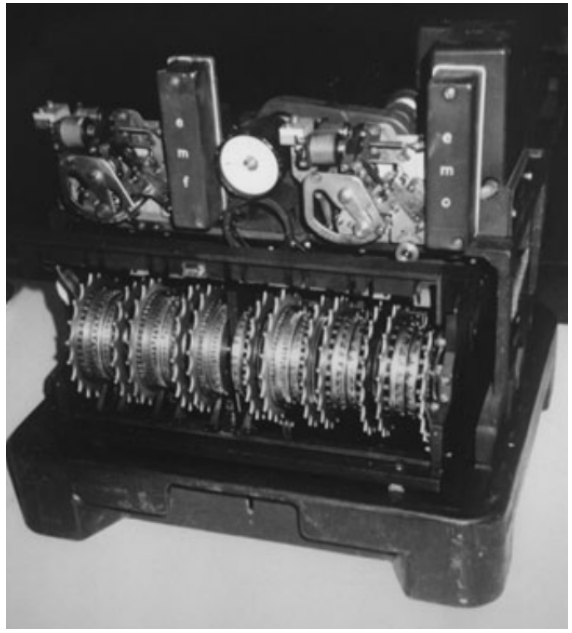


Sortie sous forme de bande perforée d'un flux de téléscripteur.

Chaque colonne correspond à une lettre, les petits trous au centre servent à l'entrainement de la bande.

La machine de Lorenz

Rajoute un système de codage/décodage en temps réel des 5 flux binaires.



Le système de codage est constitué par un système de 12 roues codeuses.
A la différence de enigma, aucune machine et aucune documentation sur le fonctionnement n'ont été capturées. Toute la cryptanalyse vient d'une étude logique des signaux interceptés.

La machine de Lorenz

- Les différentes roues sont activées par un moteur et ont respectivement 43, 47, 51, 53, 59, 37, 61, 41, 31, 29, 26, 23 positions. Pourquoi ce choix de nombres ?
- Les roues de 1 à 5 sont appelées les roues χ, les roues 6 et 7 sont les roues μ (moteur), les 5 dernières les roues ψ.
- La roue 1 a 43 contacts électriques, qui peuvent être soit conducteurs (signal 1), soit non conducteur (signal 0). De même pour chacune des autres roues.
- Le codage des lettres se fait par ou exclusif (XOR) sur chaque bit. Ainsi, si on entre la lettre M, qui correspond à 00111

signal en clair	0	0	1	1	1
signal χ	1	0	1	1	0
signal ψ	0	1	1	0	1
signal crypté	1	1	1	0	0

il sort donc la chaîne 11100, qui correspond à la lettre Q.

La machine de Lorenz

- Chaque roue χ avance d'un cran à chaque fois.
- Les 2 roues μ produisent aussi par XOR un signal qui vaut 0 ou 1.
- Si le signal μ est 1, les roues ψ avancent toutes les cinq d'un cran, sinon elles restent toutes immobiles.
- L'ensemble du système est une sorte de code de Vernam, avec une clé pseudo-aléatoire de période

  $$43 * 47 * 51 * 53 * 59 * 37 * 61 * 41 * 31 * 29 * 26 * 23 \simeq 1,6\,10^{19}$$

- L'introduction des deux roues "moteur" est destinée à rendre la clé pseudo-aléatoire encore plus "aléatoire". En réalité cela a été la principale faiblesse du système.

Exploitation d'une erreur grossière

- Un opérateur a envoyé un premier message de plus de 4000 caractères, mais le signal a été mal reçu par le destinataire.
- Il renvoie donc le même message une deuxième fois, avec les mêmes réglages de la machine, mais, par impatience, il utilise des abbréviations.
- Il a donc envoyé deux messages P et P' (P pour plaintext) , codés avec la même clé C, qui ont produit des cryptogrammes $Z = P \oplus C$ et $Z' = P' \oplus C$.
- Les crytanalystes alliés ignorent P, P' et C, mais ont intercepté Z et Z'. Ils calculent alors :

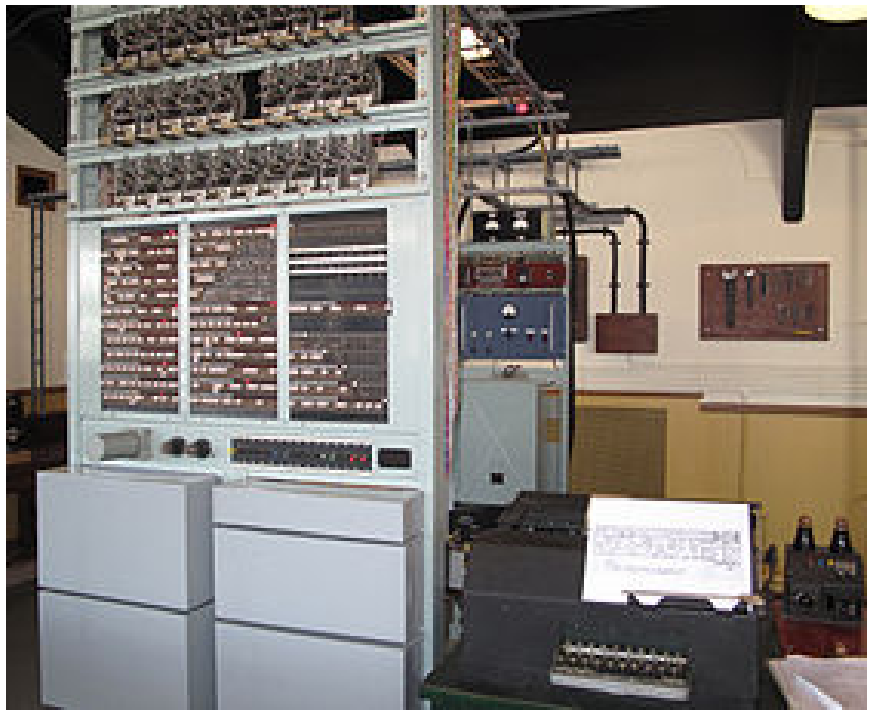
$$Z \oplus Z' = (P \oplus C) \oplus (P' \oplus C) = P \oplus P'$$

Exploitation d'une erreur grossière

- Connaissant $P \oplus P'$, ils en en déduisent par des extrapolations linguistiques P et P'.
- Connaissant alors $Z = P \oplus C$ et P, on peut en déduire C, en calculant $Z \oplus P$. Les cryptanalystes disposent maintenant d'une clé de plus de 4000 caractères !
- Par une analyse extrèmement fine des répétitions dans cette clé, il en déduisent la structure interne de la machine de Lorenz, uniquement par une analyse logique, ce qui est une performance exceptionnelle.

The British Tunny

Ce travail de rétro-ingénierie aboutit à la fabrication d'une machine ayant les même fonctionnalités que la machine de Lorenz, mais construite avec une technologie entièrement différente (celle des centraux téléphoniques) :



Déchiffrement du code Lorenz

- Même si Bletchley Park connait maintenant la structure du code Tunny, les réglages de chacune des douze roues de la machine sont changés régulièrement. Il faut donc encore être capable de décoder les messages, sans connaitre ces réglages journaliers.
- Le flux codé est relié au flux en clair par :

$$Z = P \oplus \chi \oplus \psi$$

  La statégie est de démêler le χ du ψ.
- On utilise le fait que, par la structure de la machine, un 0 dans le flux ψ est plus souvent suivi par 0 que par 1, et de même un 1 est plus souvent suivi par un 1 que par un 0. autrement dit le flux ψ ne vérifie pas les caractéristiques d'un signal aléatoire.

Déchiffrement du code Lorenz

- Observer attentivement les liens entre le flux Z et le flux $\overline{Z}$, obtenu en décalant Z d'une lettre.
- Suite de calculs faciles, mais longs et répétitifs.

Déchiffrement du code Lorenz

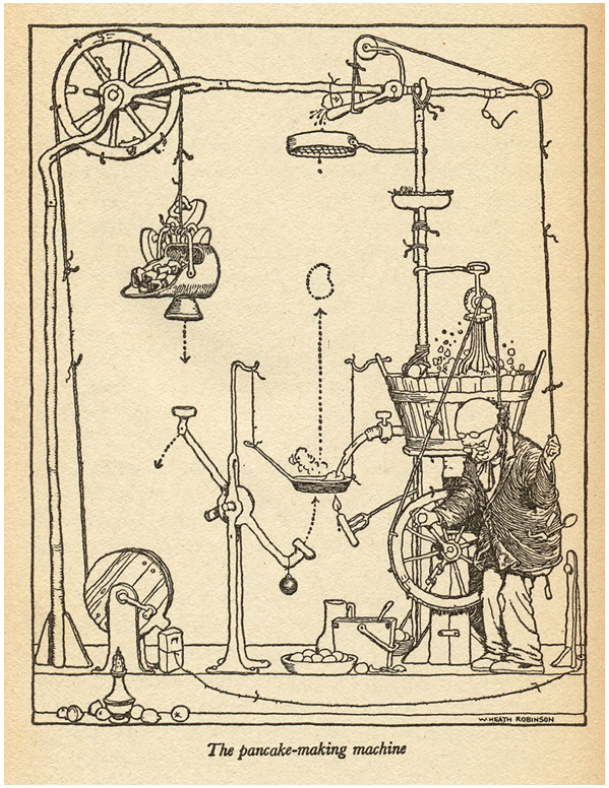
- Observer attentivement les liens entre le flux Z et le flux $\overline{Z}$, obtenu en décalant Z d'une lettre.
- Suite de calculs faciles, mais longs et répétitifs.
- D'où la nécessité de mécaniser ces calculs, par l'introduction de machines dédiées
  - Heath-Robinson
  - Colossus

Les machines Heath-Robinson

- Machines mécaniques/optiques à bandes perforées destinées à détecter les répétitions dans les flux de données.

Les machines Heath-Robinson

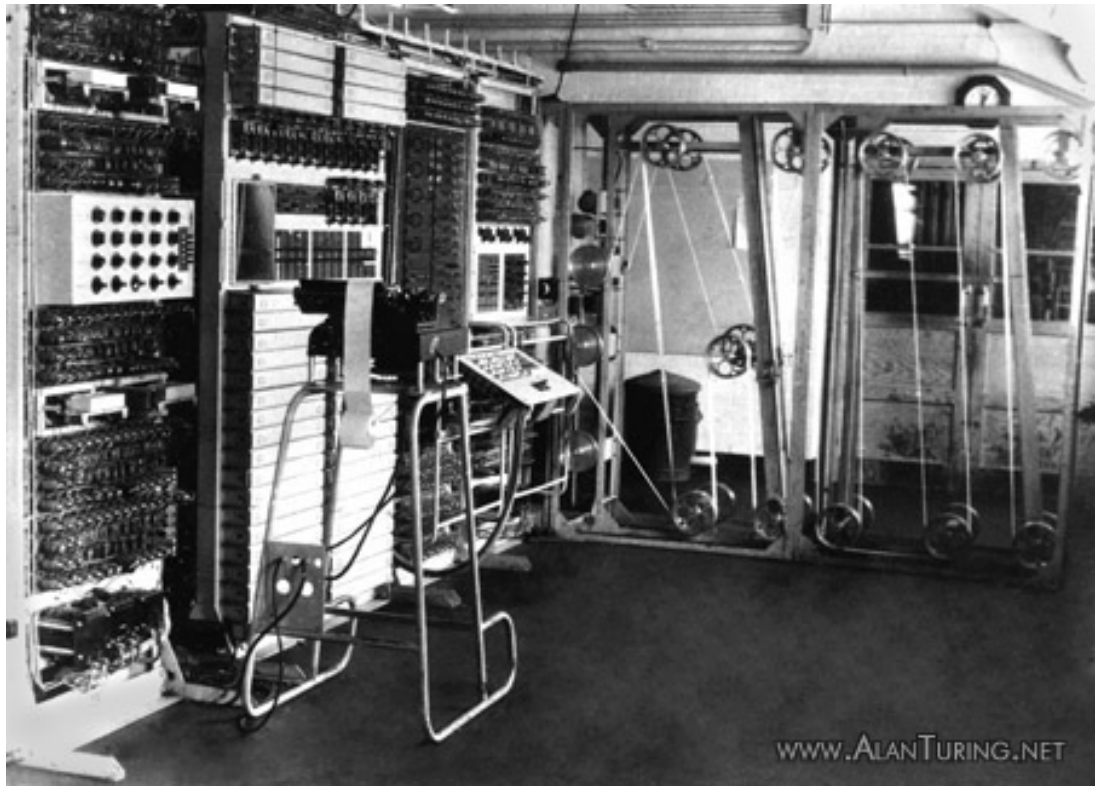
- Machines mécaniques/optiques à bandes perforées destinées à détecter les répétitions dans les flux de données.
- Dénommées ainsi du nom d'un illustrateur britannique célèbre pour ses dessins de machines d'une complexité absurde



The pancake-making machine

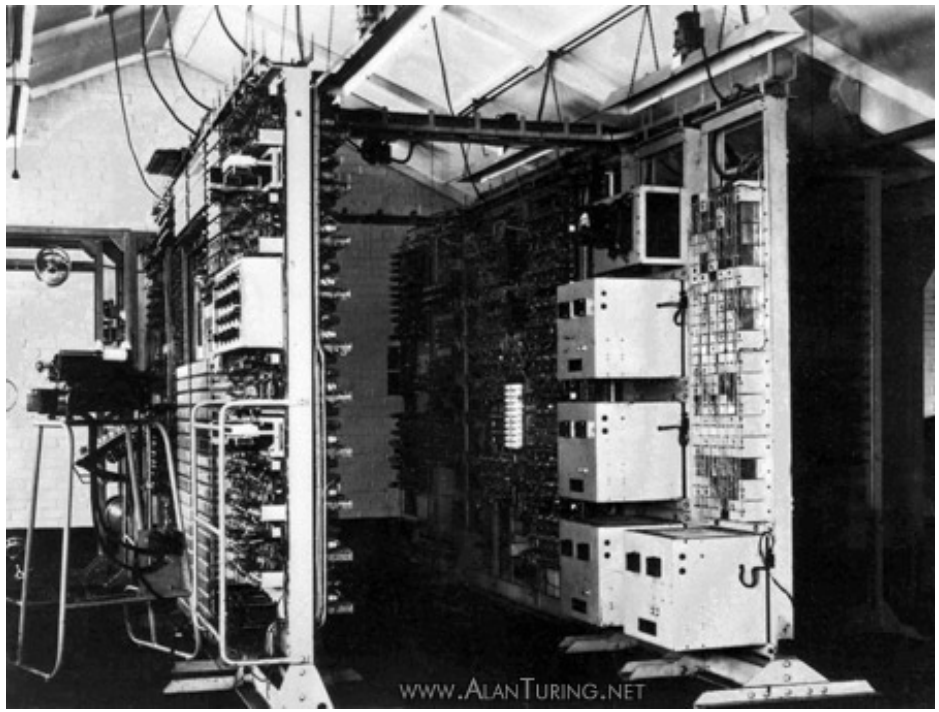
Colossus

- Compare un flux de données venant d'une bande perforée et un flux fabriqué électroniquement et établit des statistiques de concordance.
- Architecture à base de lampes à vide.
- Vitesse de la bande perforée : 5000 caractères/seconde



Colossus

- Ne devait jamais être arrêté sous peine de ne pas redémarrer (lampes à vide)
- Programmation par des interrupteurs à deux positions
- C'est un calculateur paramétrable physiquement, mais pas encore un ordinateur au sens actuel.



Importance historique

- Le déchiffrement du code Tunny a permis aux anglais d'être au courant de l'opération "Citadelle" deux mois avant son lancement. Il s'agissait pour les allemands d'une immense offensive destinée à reprendre l'avantage sur les russes après la défaite de Stalingrad.

Importance historique

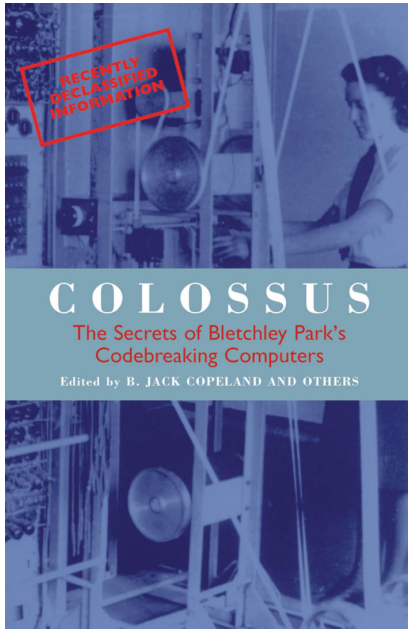
- Le déchiffrement du code Tunny a permis aux anglais d'être au courant de l'opération "Citadelle" deux mois avant son lancement. Il s'agissait pour les allemands d'une immense offensive destinée à reprendre l'avantage sur les russes après la défaite de Stalingrad.
- Churchill s'est opposé à ce qu'on communique cette information aux soviétiques.

Importance historique

- Le déchiffrement du code Tunny a permis aux anglais d'être au courant de l'opération "Citadelle" deux mois avant son lancement. Il s'agissait pour les allemands d'une immense offensive destinée à reprendre l'avantage sur les russes après la défaite de Stalingrad.
- Churchill s'est opposé à ce qu'on communique cette information aux soviétiques.
- Mais les soviétiques avaient un espion au sein de Bletchley Park, et ont pu ainsi masser suffisamment de troupes pour mettre en échec l'offensive allemande (bataille de Koursk, juillet-aout 1943).

Quelques références

- Wikipedia
- http ://www.ellsbury.com/enigmabombe.htm
- http ://www.rutherfordjournal.org/article030109.html
- Un livre complet sur colossus



Merci pour votre attention